4

AlliedWare Plus™ Version 2.1.2
AT-9000 Layer 2-4 Gigabit Ethernet EcoSwitches
Software Release Notes

Please read this document before you begin to use the management software. The document has the following sections:

Caution:
The software described in this document contains certain cryptographic functionality and its export is restricted by U.S. law. As of this writing, it has been submitted for review as a “retail encryption item” in accordance with the Export Administration Regulations, 15 C.F.R. Part 730-772, promulgated by the U.S. Department of Commerce, and conditionally may be exported in accordance with the pertinent terms of License Exception ENC (described in 15 C.F.R. Part 740.17). In no case may it be exported to Cuba, Iran, Iraq, Libya, North Korea, Sudan, or Syria. If you wish to transfer this software outside the United States or Canada, please contact your local Allied Telesis sales representative for current information on this product’s export status.

Supported Platforms

Version 2.1.2 of the AlliedWare Plus™ Management Software is supported on these switches:

- ❒ AT-9000/28
- ❒ AT-9000/28SP
- ❒ AT-9000/52

This version supports the following SFP modules:

- ❒ AT-SPTX (Supported only at a speed of 1G.)

- AT-SPEX
- AT-SPSX
- AT-SPFX/2
- AT-SPFX/15
- AT-SPLX10
- AT-SPLX40
- AT-SPZX/80
- AT-SPBD10-13
- AT-SPBD10-14
- AT-SPFXBD-LC-13
- AT-SPFXBD-LC-15

What's New in Version 2.1.2

- The new VLAN stacking feature allows metro Ethernet networks to tag packets with unique 802.1Q headers to create encapsulated connections through the core, for multiple customer edge VLANs.
- The web browser interface has been significantly enhanced to allow for more system monitoring and control.
- The command line interface has been enhanced to conform to the Allied Telesis CLI standard.
- The BANNER EXEC, BANNER MOTD, and BANNER LOGIN commands now support messages with carriage returns.
- You may now use the Telnet client from local and Telnet management sessions, whereas before you could only use it from local management sessions.
- The switch now supports digital diagnostic monitoring (DDM) for those SFP modules that support it. The messages are entered in the event log.
- Port descriptions now support up to 80 characters.

Introduction to Upgrading the Switch

You should determine the current version of the management software on the switch before updating it. The current management software will determine the appropriate upgrade process:

- If the switch has the AT-S100 Management Software, refer to the *AlliedWare Plus Version 2.1.1 Software Release Notes* for the upgrade instructions. You may update the unit directly to AlliedWare Plus version 2.1.2 from the AT-S100 Management Software, and skip AlliedWare Plus version 2.1.1.
- If the switch already has AlliedWare Plus, you may upgrade it to version 2.1.2 using either the command line interface or web browser interface. These software release notes contain the procedure for updating the management software using the command line interface. If you want to use the web browser interface, refer to the *AlliedWare Plus Web Browser User's Guide*.

Upgrading the AT-9000 Switch to AlliedWare Plus Version 2.1.2 from Version 2.1.1

This section contains the procedure for upgrading the switch from AlliedWare Plus Version 2.1.1 to version 2.1.2, from the command line. Here are the upgrade requirements:

- There must be a TFTP server on your network.
- The switch must be assigned an IP address. For instructions, refer to the *AT-9000 AlliedWare Plus User's Guide*.

Caution:
The upgrade process is disruptive to network operations because it resets the switch. The switch does not forward network traffic during the reset.

There are three phases to upgrading the switch:

- "Phase 1. Uploading the Active Boot Configuration File to Your TFTP Server" on page 3
- "Phase 2: Downloading the New AlliedWare Plus Version 2.1.2 Management Software" on page 4
- "Phase 3: Updating the Commands" on page 4

Phase 1. Uploading the Active Boot Configuration File to Your TFTP Server

Allied Telesis recommends uploading the active boot configuration file from the switch to your TFTP server before updating the management software on the switch. You'll use the file in phase 3 to check for v2.1.1 commands that are not compatible with v2.1.2. To upload the active boot configuration file:

1. Start the TFTP server on your network.
1. Start a local or remote management session on the switch.
2. When prompted, enter a username and password. The defaults are "manager" for the username and "friend" for the password.
3. Move to the Privileged Exec mode and enter the SHOW BOOT command to display the name of the active boot configuration file:

   ```
   awplus# show boot
   ```

   Here is an example of the information.

   ```
   Current software   : v2.1.1
   Current boot image : v2.1.1
   Backup boot image  : Not set
   Default boot config: /cfg/boot.cfg
   Current boot config: /cfg/sw2bldg2.cfg (file exists)
   ```

   The name of the active boot configuration file is displayed in the "Current boot config" line.
4. Use the COPY command to upload the boot configuration file from the switch to the TFTP server. Here is the format of the command:

   copy flash tftp *ipaddress filename*.cfg

   The IPADDRESS parameter is the IP address of the TFTP server. The FILENAME parameter is the name of the boot configuration file you want to upload from the switch to TFTP server. The filename extension must be ".cfg" for boot configuration files. The filename cannot contain spaces.

This example of the command uploads the boot configuration file “sw2bldg2.cfg to a TFTP server that has the IP address 149.182.34.15:

```
awplus# copy flash tftp 149.182.34.15 sw2bldg2.cfg
```

5. Go to Phase 2.

Phase 2: Downloading the New AlliedWare Plus Version 2.1.2 Management Software

To upgrade the switch to AlliedWare Plus Version 2.1.2 from AlliedWare Plus Version 2.1.1:

1. Store the AlliedWare Plus Version 2.1.2 Management Software on the TFTP server on your network.
2. If you have not already started the TFTP server, start it now.
3. If you have not already started a local or remote management session on the switch, start a session now.
4. Use the ENABLE command to move to the Privileged Executive mode.

   ```
   awplus> enable
   awplus#
   ```

5. Use the COPY command to download the AlliedWare Plus Version 2.1.2 Management Software from the TFTP server to the switch. Here is the format of the command:

   `copy tftp flash` *`ipaddress filename`*

   The IPADDRESS parameter specifies the IP address of the TFTP server on your network. The FILENAME parameter specifies the filename of the AlliedWare Plus Version 2.1.2 Management Software stored on the TFTP server. The extension must include the “.img” extension. The name cannot contain spaces or special characters.

   In this example, the IP address of the TFTP server is 149.157.18.78 and the name of the management software file is “ats-9000-2.1.2.img:”

   ```
   awplus# copy tftp flash 149.157.18.78 ats-9000-2.1.2.img
   ```

   After receiving the file from the TFTP server, the switch writes it to flash memory and resets. The entire process takes several minutes. The switch is running the new software after it completes the reset.
6. Establish a new management session with the switch.
7. Enter the Privileged Exec mode and enter the WRITE command to same the configuration.

   ```
   awplus> enable
   awplus# write
   ```

8. Go to Phase 3.

Phase 3: Updating the Commands

A few commands have changed from v2.1.1 to v2.1.2. If the switch encountered any of these commands in its boot configuration file when it reset, it skipped over them to remove them from its running configuration. To complete the upgrade procedure, you should print out the boot configuration file you uploaded to your TFTP server in Phase 1, and examine it for any of the modified commands. The modified commands are described here:

- BANNER EXEC and BANNER MOTD Commands - The formats of these commands, which are used to create the User Exec and Privileged Exec modes banner and message-of-the-day banner, have changed in v2.1.2. Where before a command and its banner message were included on the same line, they are now entered separately. The new formats are:

  ```
  banner exec
  banner motd
  ```

After you enter a banner command, the prompt “Type CTRL/D to finish” is displayed on your screen, at which point you may enter a banner message of up to 50 characters for the User Exec and Privilege Exec modes banner and 100 characters for the message-of-the-day banner. Spaces and special characters are allowed. When you are finished entering a message, hold down the CTRL key and type D to return to the command prompt in the Global Configuration mode. To test the banner for the User Exec and Privilege Exec modes, return to the Privileged Exec mode and issue the CLEAR SCREEN command. To test the message-of-the-day banner, log out and log in again.

This example creates the User Exec and Privilege Exec modes banner “Engineering Switch Building 12:”

```
awplus> enable
awplus# configure terminal
awplus(config)# banner exec
Type CNTL/D to finish
Engineering Switch Building 12
awplus(config)#
```

This example creates the message-of-the-day banner “Updated November 12, 2010:”

```
awplus> enable
awplus# configure terminal
awplus(config)# banner motd
Type CNTL/D to finish
Updated November 12, 2010
awplus(config)#
```

- LOG BUFFERED Command - The function and format of the LOG BUFFERED command has not changed, but the FAN_CTRL option is no longer supported. If the command and option are in the backup boot configuration file, reenter the command on the switch, omitting the option.
- FILTERING Command - This command, which In v2.1.1 allowed you to block ingress broadcast, multicast, or unknown unicast packets on ports, is not supported in version 2.1.2. There is no equivalent v2.1.2 command.
- CLOCK TIMEZONE Command - If the switch is using an SNTP or NTP server as the source of its date and time, you have to reenter the CLOCK TIMEZONE command because its format has changed. You may now specify both hours and minutes to identify the difference between local time and UTC, whereas before the command only accepted hours. The new format of the command is:

  `clock timezone +`*`hh:mm`*`|-`*`hh:mm`*

  HH are hours in the range of -12 to +12 and MM are minutes in the range of 00 to 60. The offset must include a plus or minus sign. You must include both the hours and minutes, and both values must have two digits. The example sets the UTC offset to +2 hours:

  ```
  awplus> enable
  awplus# configure terminal
  awplus(config)# clock timezone +02:00
  ```

  The example sets the UTC offset to -8 hours, 15 minutes:

  ```
  awplus> enable
  awplus# configure terminal
  awplus(config)# clock timezone -08:15
  ```

- SET SFLOW COLLECTOR IP Command - In v2.1.1 this command in the Port Interface mode was used to identify the sFlow collector that was to be the recipient of packet data from a port. This command is not supported in v2.1.2 because you may specify only one sFlow collector for the switch. The collector is identified with the SFLOW COLLECTOR IP command in the Global Configuration mode.
- IP ACCESS-GROUP command - The function of this command, which is used to assign access control lists (ACLs) to ports, has not changed in v2.1.2, but the IP keyword has been removed, shortening the command to just ACCESS-GROUP. To reapply the ACLs to the ports, it will be necessary to reenter the command in the Port Interface modes of the appropriate ports. To do this, examine the backup configuration file for any IP ACCESS-GROUP commands and then reenter the same commands, but without the IP keyword, in the Port Interface modes of the affected ports.

Troubleshooting the Upgrade Procedure

If you have a problem downloading the management software to the switch from your TFTP server, here are a few suggestion on how to resolve it:

- Check that the TFTP server on your network is active.
- Use the SHOW IP INTERFACE command in the User Exec or Privileged Exec mode to verify that the switch has an IP address.
- Use the PING command in the Privileged Exec mode to check for an active link between the switch and your TFTP server.
- Verify that you entered the COPY command correctly. Be sure to include the ".img" extension in the filenames of the management software file.
- If you are using a TFTP server that is case sensitive, be sure to use upper and lowercase characters when specifying filenames in the commands.
- Check that the management software file is stored in the correct directory on the TFTP server.

Operational Notes

- The speed of the AT-SPFX/2 and AT-SPFX/15 modules has to be manually set to 100Mbps with the SPEED command. This example of the command configures the speed of the AT-SPFX/2 or AT-SPFX/15 module in slot 1 of an AT-9000/28SP Switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# speed 100
```

- The assignment of an IPv6 management address to the switch must be performed manually using the IPV6 IPADDRESS command, because the switch cannot obtain an IPv6 address with stateless autoconfiguration or from a DHCP6 server.
- You cannot use the web browser interface to configure these features:
  - Access control lists
  - Enhanced stacking
  - Quality of Service
  - SNMP
  - Voice VLANs

— VLAN stacking

Use the command line interface to configure these features.

- The web browser interface has been tested and found to be compatible with the following web browsers:
  - Microsoft Internet Explorer 7 and 8
  - Mozilla Firefox 3.6.3
  - Apple Safari 4.0.5

Note:
If you are using Explorer 8 web browser and the pull-down menus in the switch's web browser interface do not work, open the Internet Options window in the web browser, select the Security tab, and set the custom settings to medium-high. Then refresh your page.

- You cannot change the configuration of a port, such as its VLAN assignment, after it is added to a static or an LACP trunk. The configuration of a port must be set before it is added to a trunk.
- You can create up to 4096 VLANs on the switch, but only 255 VLANs can be active at a time.
- Changing the SNMPv3 engineID value is not recommended because the SNMP server on the switch may fail to operate properly.

Resolved Issues

The following issues were resolved in this release.

- SNMP server: The SNMP server stopped working during SNMP walks. (8222)
- SNMP server: The SNMP server stopped working if you activated the HTTP or HTTPS server and reset the switch. (8148)
- SNMP and Telnet servers: A memory leak problem in the SNMP and Telnet servers caused the switch to reset after forty management sessions. (8318)
- SNMP server: Access control lists created with SNMP were deleted by the switch. (8651)
- SNMP server: The switch displayed debug messages during local management sessions if there was also an active SNMP session. (8646)
- SNMP server: The switch periodically displayed an IPC_TIMEOUT_ERROR message when it was managed with SNMP. (8201)
- SNMP traps: The switch sent SNMP traps even when they were disabled. (8650)
- Port configuration: The SHOW INTERFACE command displayed negative numbers. (8263)
- SNTP client: The CLOCK TIMEZONE command did not accept minutes in its format. (8145)
- SNTP client: The SHOW NTP ASSOCIATIONS command did not display the UTC offset correctly. (8196)
- SNTP client: System time drifted forward if it was set by an NTP or SNTP server. (8612)
- SNTP client: The NTP client did not synchronize properly with the Microsoft Windows XP Time server. (8626)
- SNTP client: The client periodically caused the switch to stop forwarding network traffic. (8637)

- Port-based and tagged VLANs: You could not change a port from the trunk mode to the access mode. (8319)
- IGMP snooping: The switch did not properly register IGMP queries and reports. (8301)
- sFlow client: The switch stopped forwarding traffic if the sFlow client was active on more than twelve ports. (8236)
- STP and enhanced stacking: The switch stopped forwarding traffic if both STP and enhanced stacking were activated. (8246)
- STP: The switch would reset if the spanning tree protocol detected a loop in the network topology. (8094)
- STP: The spanning tree protocol stopped sending BPDUs when the SNTP client synchronized system time with an NTP or SNTP server. (8605)
- STP: The spanning tree SHOW commands did not display the settings for BPDU guard, root guard, portfast and other parameters. (8639)
- RADIUS client: The RADIUS acronym was misspelled in the web browser interface. (8625)
- GVRP: Dynamic GVRP VLANs were saved as static VLANs in the active boot configuration file. They are now relearned when the unit is reset. (8321)
- ACLs: The copy-to-mirror option did not work. (8675)
- LACP: The switch disabled the remaining ports of an eight port LACP trunk if the connections were lost on four of the ports. (8599)
- LACP: LACP trunks caused the switch to display a “Kernel paging request” error message and to reset. (8618)
- LACP: The switch would reset if a port in an LACP trunk that had 20 or more ports lost its connection.(8638)
- LACP: There was a delay in the resumption of traffic on LACP connections that changed link states. (8619)
- LACP: Fluctuating connections in LACP trunks resulted in IPC errors. (8622)
- Telnet server: You could not overwrite existing encryption keys from a Telnet management session. (8616)
- SSH server: You could start a remote SSH management session without having to enter a username. (8712)
- SSH server: The switch did not properly timeout inactive remote SSH management sessions.

Known Issues

There are no known issues in this release.

Changes to the AlliedWare Plus Command Line User's Guide

Here are the main changes to the *AlliedWare Plus Command Line User's Guide* for version 2.1.2.

Table 1. Changes to the AlliedWare Plus Management Software User's Guide for Version 2.1.2

Chapter	Description
Chapters 5 and 6: Basic Switch Management	The formats of the BANNER EXEC and BANNER MOTD commands in the Global Configuration mode have changed such that the banner messages are now entered separately from the command.
	The HOSTNAME command now accepts special characters, but not spaces or quotation marks.
	The command reference chapter now includes the SYSTEM TERRITORY command, for designating the territory where the switch is installed.
Chapters 7 and 8: Port Parameters	Revision A of the user's guide incorrectly stated that you had to disable Auto-Negotiation to manually set the speed, duplex mode and MDI/MDI-X settings on the ports. Revision B states that all three settings may be set independently of each other. For example, you could configure a port such that its speed is set manually to 100 Mbps, its duplex mode to Auto-Negotiation, and its wiring configuration to MDI.
	The FILTERING and NO FILTERING commands described in Revision A of the guide are no longer supported on the switch.
Chapters 11 and 12: Simple Network Time Protocol Client	The format of the CLOCK TIMEZONE command has been modified to accept minutes in the UTC offset, which the switch uses to convert UTC time into local time.
Chapter 20: Multicast Commands	New commands for blocking unknown multicast packets.
Chapters 26 and 27: File Transfers	You may no longer use Zmodem to download new management software to the switch. That management task must be performed with TFTP. You may use Zmodem to upload or download boot configuration files, encryption key certificates or requests, and diagnostic text files.
Chapter 29: Event Log Commands	The SHOW LOG command no longer supports the FAN_CTRL module.
Chapters:50 and 51: VLAN Stacking	VLAN stacking is a new feature.

Table 1. Changes to the AlliedWare Plus Management Software User's Guide for Version 2.1.2

Chapter	Description
Chapter 52: MAC Address-based Port Security	Revision A of the user's guide stated in Guidelines that this type of port security was not supported on optional GBIC, SFP, or XFP modules. Revision B states that MAC address-based port security is supported on SFP transceivers, the only type of transceivers AT-9000 switches support.
Chapters 59 and 60: sFlow Agent	Revision A of the user's guide stated you could define the IP addresses of up to four sFlow collectors. The switch actually supports the IP address of just one collector. This is corrected in Revision B.
Chapters 67 and 68: Access Control Lists (ACLs)	Revision A stated that a port that had more than one ACL performs them according to their ID numbers, in ascending order. ACLs are actually performed in the order in which they are applied to a port. This is corrected in Revision B.
	The IP ACCESS-GROUP command, which is used to assign ACLs to ports, has been shortened to ACCESS-GROUP command.
	The previous version of the user's guide stated that ACLs without the VLAN parameter applied to both tagged and untagged packets. That is incorrect. ACLs without the VLAN parameter apply only to untagged packets.
Chapters 70 and 71: Local Manager Accounts	This version of the management software has a NO SERVICE PASSWORD-ENCRYPTION command that disables password encryption of local manager accounts. In the previous version, you could not disable password encryption after you had activated it.
	Previously, manager accounts with a privilege level of 1 could access all of the command modes except when command mode restriction was activated, in which case they were restricted to the User Exec mode, unless they knew the special password. In this release, command mode restriction is always activated to prevent managers who have a privilege level of 1 and do not know the special password from accessing any mode beyond the User Exec mode.
Chapter 74 and 75: Telnet Client	In the previous release the Telnet client could only be used from local management sessions of the switch. In this release you may use it from local and Telnet management sessions.

Table 1. Changes to the AlliedWare Plus Management Software User's Guide for Version 2.1.2

Chapter	Description
Chapter 77: SSH Server Commands	The following commands documented in revision A are not in the firmware and have been removed from revision B: ❒ SSH SERVER LOGIN-TIMEOUT Command ❒ SSH SERVER MAX-STARTUPS Command ❒ SSH SERVER SESSION-TIMEOUT command Administrators may use the EXEC-TIMEOUT command in place of the SSH SERVER SESSION-TIMEOUT command to set the session timeout timers.

Contacting Allied Telesis

This section provides Allied Telesis contact information for technical support as well as sales or corporate information.

Online Support

You can request technical support online by accessing the Allied Telesis Knowledge Base: **www.alliedtelesis.com/support/kb.aspx**. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

Email and Telephone Support

For Technical Support via email or telephone, refer to the Support & Services section of the Allied Telesis web site: **www.alliedtelesis.com**. Select your country from the list displayed on the website. then select the appropriate menu tab.

Warranty

For hardware warranty information, refer to the Allied Telesis web site: **www.alliedtelesis.com/support/warranty**.

Returning Products

Products for return or repair must first be assigned a return materials authorization (RMA) number. A product sent to Allied Telesis without an RMA number will be returned to the sender at the sender's expense. For instructions on how to obtain an RMA number, go to our web site at **www.alliedtelesis.com** and then select Support and Replacement Services.

Sales or Corporate Information

You can contact Allied Telesis for sales or corporate information through our web site: **www.alliedtelesis.com**.

Management Software Updates

New releases of management software for our managed products are available on our Allied Telesis web site at **http://www.alliedtelesis.com/support/software**.